(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
25. Juli 2002 (25.07.2002)

PCT

(10) Internationale Veröffentlichungsnummer
WO 02/057905 A1

(51) Internationale Patentklassifikation[7]: G06F 9/30

(21) Internationales Aktenzeichen: PCT/DE02/00110

(22) Internationales Anmeldedatum:
16. Januar 2002 (16.01.2002)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
101 01 956.4 17. Januar 2001 (17.01.2001) DE

(71) Anmelder *(für alle Bestimmungsstaaten mit Ausnahme von US)*: **INFINEON TECHNOLOGIES AG** [DE/DE]; St.-Martin-Str. 53, 81669 München (DE).

(72) Erfinder; und

(75) Erfinder/Anmelder *(nur für US)*: **HARTLIEB, Heimo** [AT/AT]; Rudersdorferstr. 164, A-8055 Graz (AT). **SEDLAK, Holger** [DE/DE]; Neumünster 10a, 85658 Egmating (DE). **KLUG, Franz** [AT/DE]; Ottobrunner Str. 17, 81737 München (DE).

(74) Anwalt: **EPPING, HERMANN & FISCHER**; Ridlerstr. 55, 80339 München (DE).

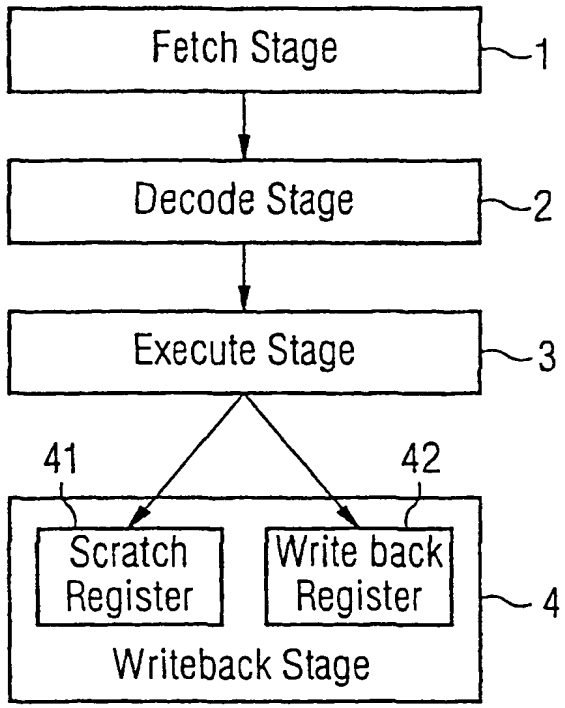
(81) Bestimmungsstaaten *(national)*: BR, CA, CN, IL, IN, JP, KR, MX, RU, UA, US.

(84) Bestimmungsstaaten *(regional)*: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) **Title:** METHOD FOR INCREASING THE SECURITY OF A CPU

(54) **Bezeichnung:** VERFAHREN ZUR ERHÖHUNG DER SICHERHEIT EINER CPU



(57) Abstract: The invention relates to a method for increasing the security of a CPU, which is characterized by using a pipeline that comprises a fetch stage (1), a decode stage (2), an execute stage (3) and a writeback stage (4), said writeback stage having at least one register (41) and at least one register (42). When the register (41) is used, the status of the CPU remains unchanged, while when the register (42) is used, the status of the CPU is changed. The inventive method is further characterized in that in the decode stage at least one randomly chosen code sequence is inserted as the dummy code sequence or filler, thereby making an attack by DPA more difficult.

(57) Zusammenfassung: Bei dem Verfahren wird eine Pipeline bestehend aus einer Ladestufe (1), einer Decodierstufe (2), einer Ausführungsstufe (3) und einer Rückspeicherstufe (4) verwendet. Die Rückspeicherstufe besitzt mindestens ein Register (41), bei dessen Benutzung keine Zustandsänderung der CPU erfolgt, und mindestens ein Register (42), bei dessen Benutzung eine Zustandsänderung der CPU erfolgt. Erfindungsgemäß wird in der Decodierstufe mindestens eine zufällig ausgewählte Codesequenz als Platzhalter-Code oder Füllsel eingefügt, womit ein Angriff durch DPA erschwert wird.

WO 02/057905 A1